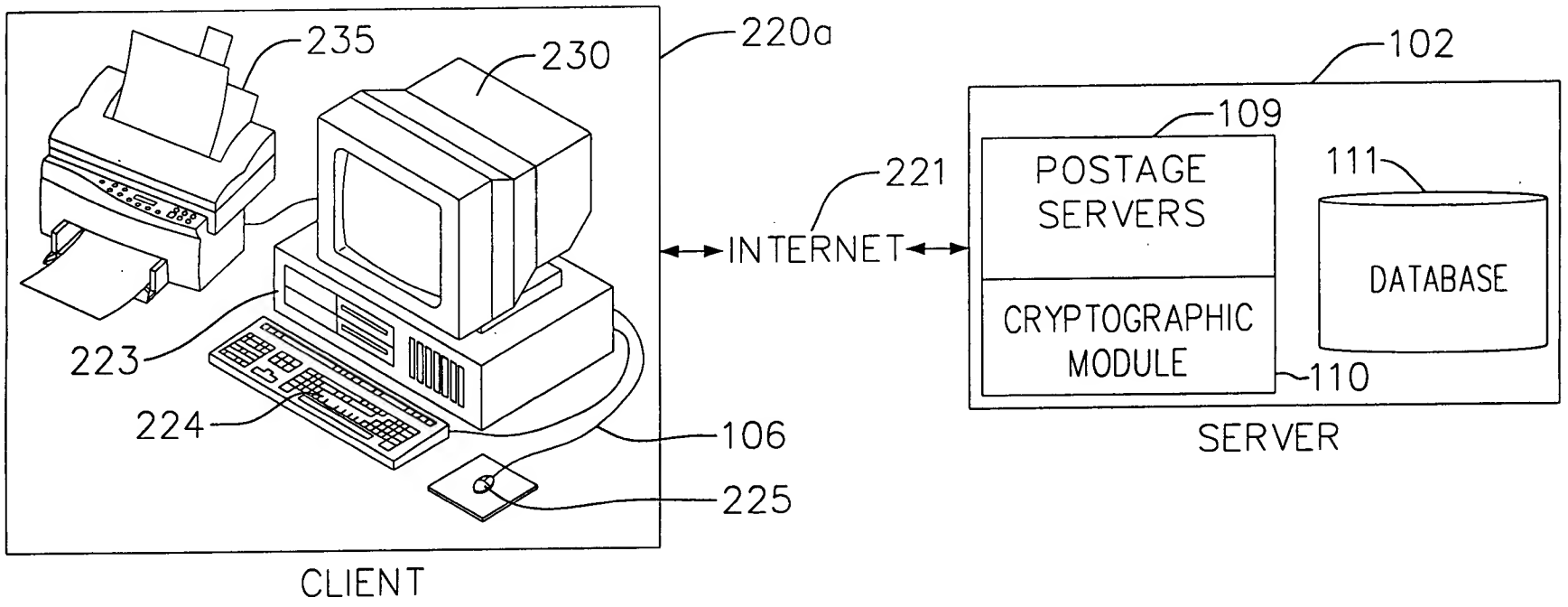
DOCTOT" EP2069600

FIG. 1



0270T' Eh20690

FIG.2

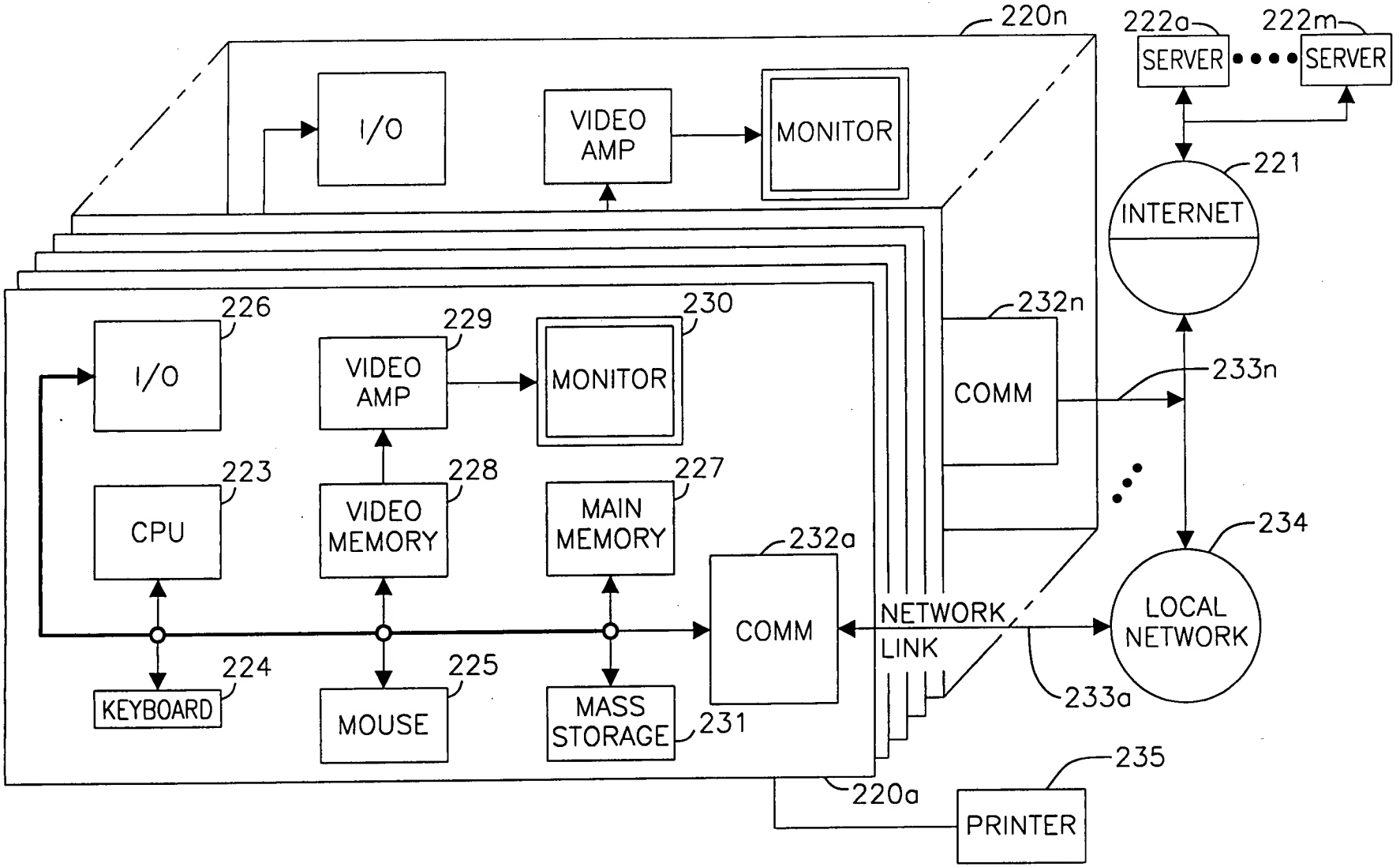


FIG. 3

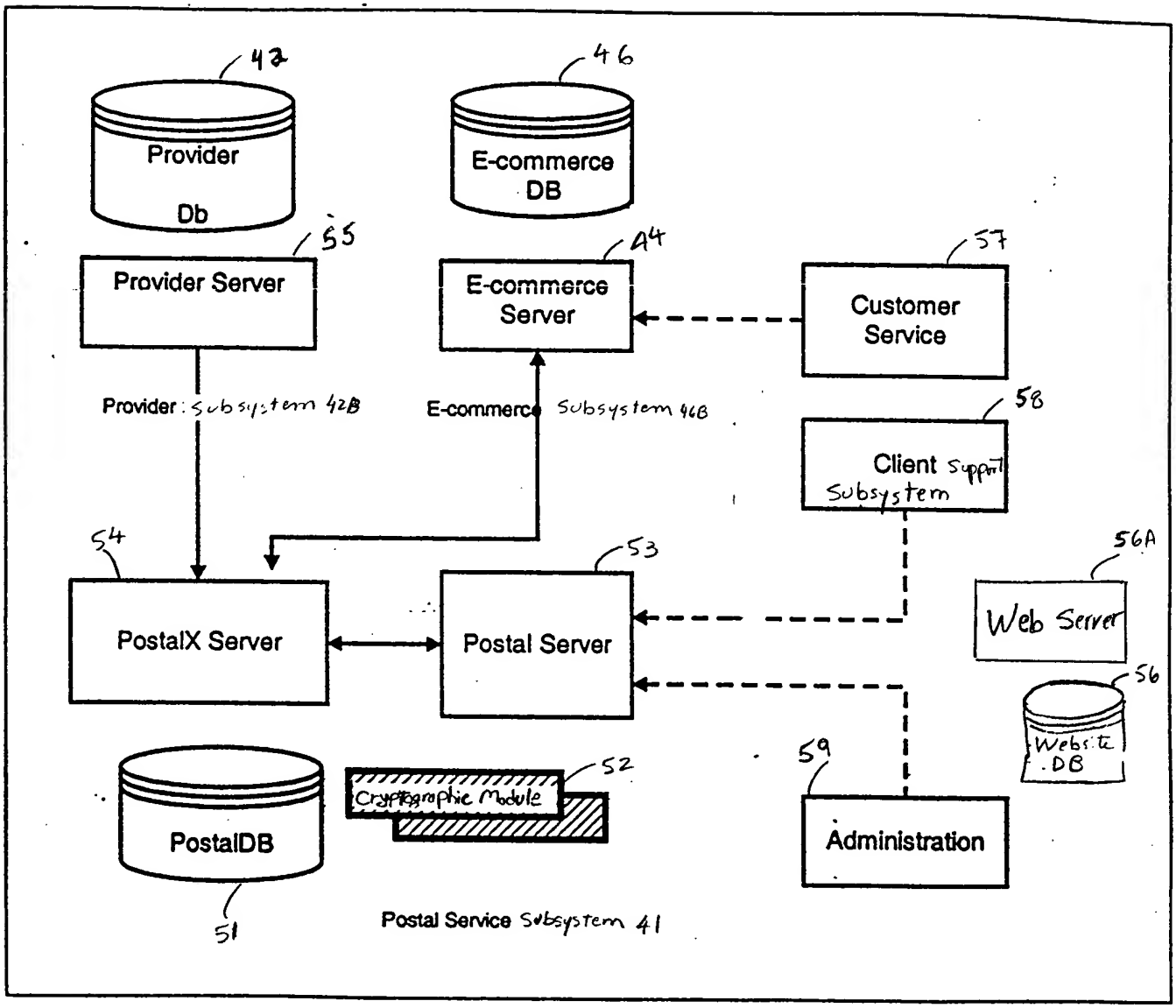

42
Provider
Db
46
E-commerce
DB
55
Provider Server
44
E-commerce
Server
57
Customer
Service
Provider Subsystem 42B
E-commerce Subsystem 46B
58
Client Support
Subsystem
54
PostalX Server
53
Postal Server
56A
Web Server
56
Website
DB
59
Administration
PostalDB
51
52
Cryptographic Module
Postal Service Subsystem 41

FIG. 4

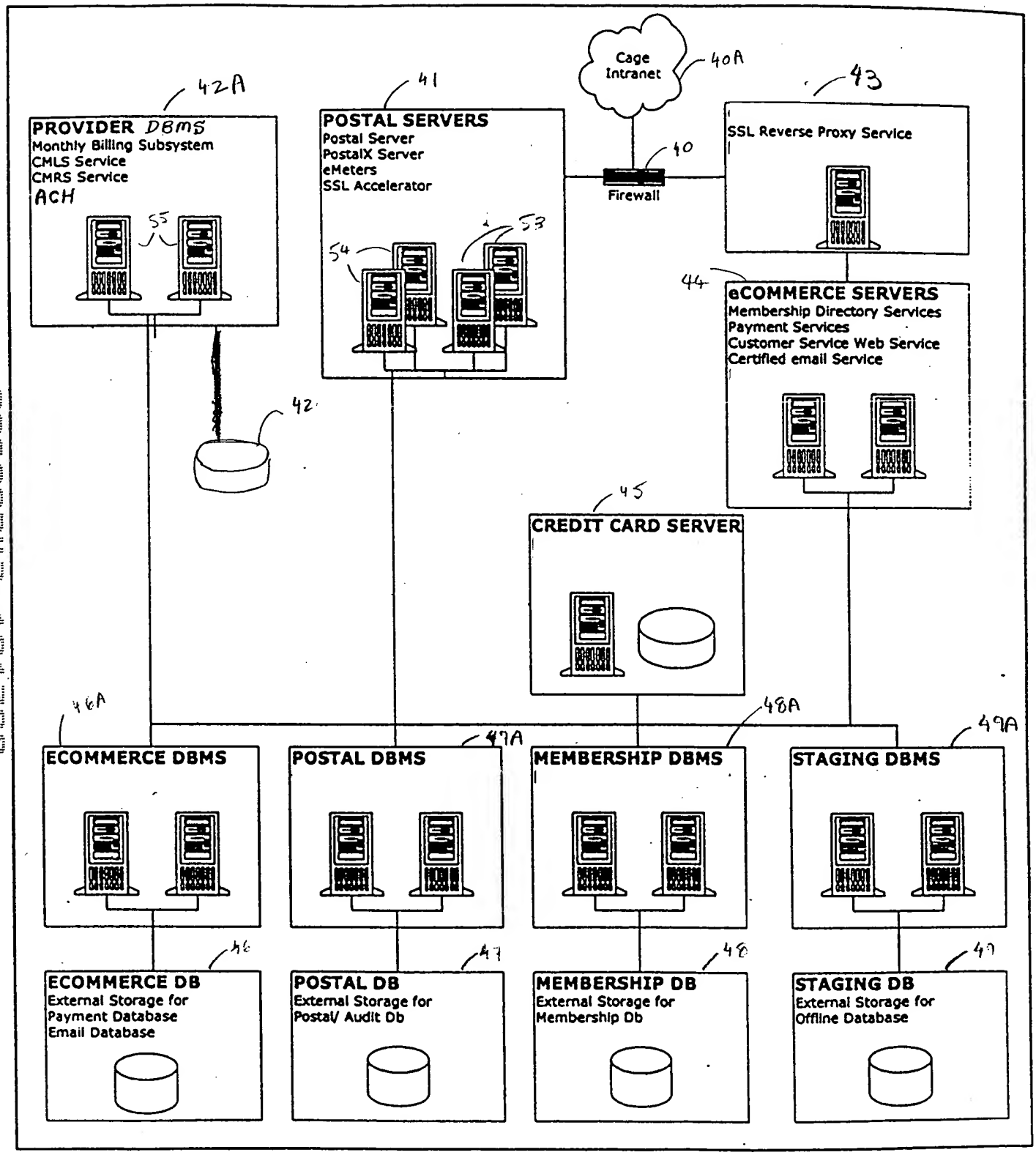

Cage
Intranet
40A
42A
41
43
PROVIDER DBMS
Monthly Billing Subsystem
CMLS Service
CMRS Service
ACH
55
POSTAL SERVERS
Postal Server
PostalX Server
eMeters
SSL Accelerator
54
53
40
Firewall
SSL Reverse Proxy Service
44
eCOMMERCE SERVERS
Membership Directory Services
Payment Services
Customer Service Web Service
Certified email Service
42
45
CREDIT CARD SERVER
46A
47A
48A
49A
ECOMMERCE DBMS
POSTAL DBMS
MEMBERSHIP DBMS
STAGING DBMS
46
47
48
49
ECOMMERCE DB
External Storage for
Payment Database
Email Database
POSTAL DB
External Storage for
Postal/ Audit Db
MEMBERSHIP DB
External Storage for
Membership Db
STAGING DB
External Storage for
Offline Database

FIG. 4A

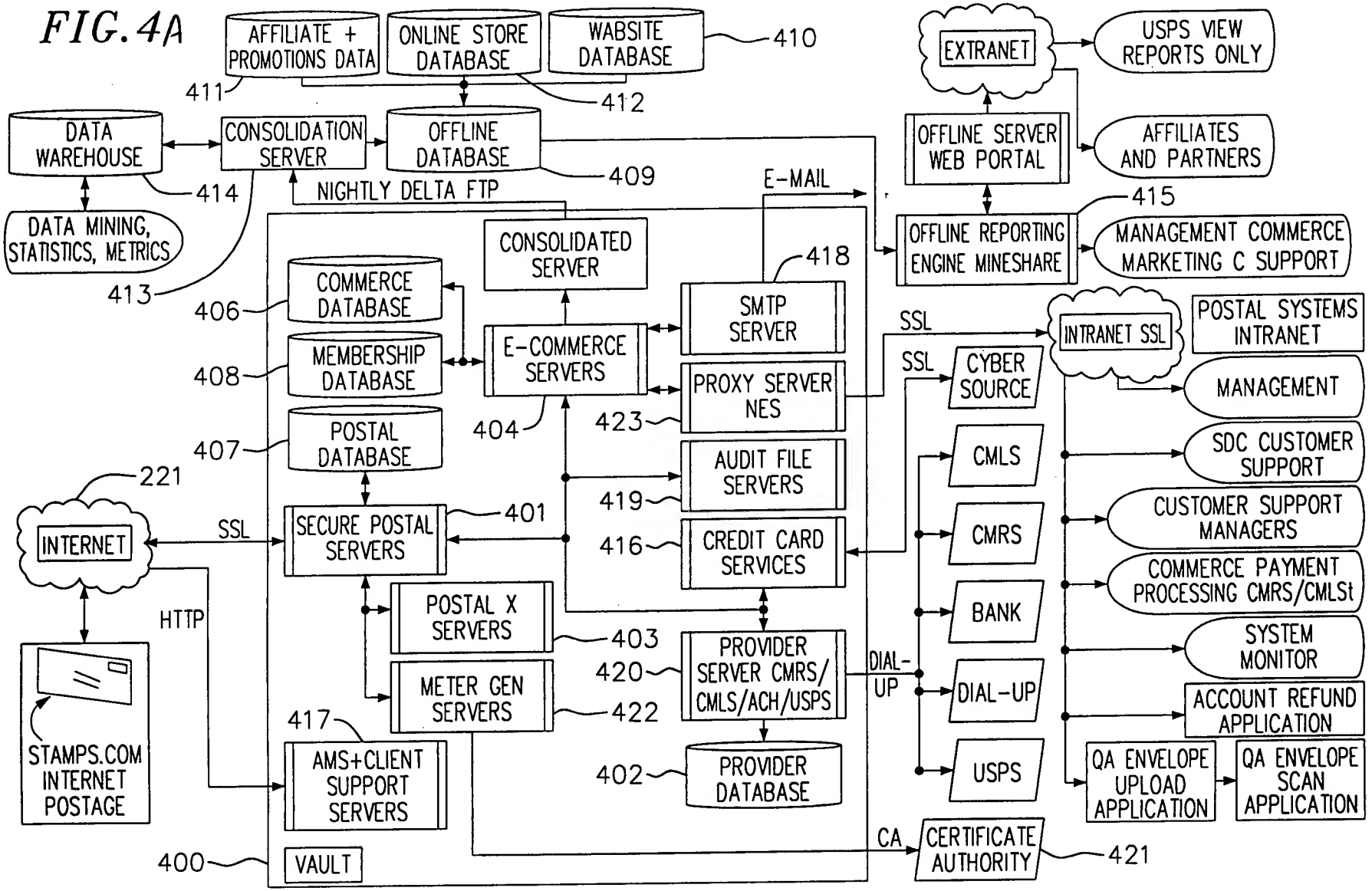

AFFILIATE + PROMOTIONS DATA
ONLINE STORE DATABASE
WABSITE DATABASE
410
411
412
DATA WAREHOUSE
CONSOLIDATION SERVER
OFFLINE DATABASE
409
414
NIGHTLY DELTA FTP
E-MAIL
DATA MINING, STATISTICS, METRICS
413
CONSOLIDATED SERVER
418
COMMERCE DATABASE
406
MEMBERSHIP DATABASE
408
POSTAL DATABASE
407
E-COMMERCE SERVERS
404
SMTP SERVER
PROXY SERVER NES
423
AUDIT FILE SERVERS
419
CREDIT CARD SERVICES
416
221
INTERNET
SSL
SECURE POSTAL SERVERS
401
HTTP
POSTAL X SERVERS
403
METER GEN SERVERS
422
420
PROVIDER SERVER CMRS/ CMLS/ACH/USPS
417
AMS+CLIENT SUPPORT SERVERS
402
PROVIDER DATABASE
STAMPS.COM INTERNET POSTAGE
400
VAULT
CA
CERTIFICATE AUTHORITY
421
EXTRANET
USPS VIEW REPORTS ONLY
OFFLINE SERVER WEB PORTAL
AFFILIATES AND PARTNERS
415
OFFLINE REPORTING ENGINE MINESHARE
MANAGEMENT COMMERCE MARKETING C SUPPORT
SSL
SSL
CYBER SOURCE
DIAL-UP
CMLS
CMRS
BANK
DIAL-UP
USPS
INTRANET SSL
POSTAL SYSTEMS INTRANET
MANAGEMENT
SDC CUSTOMER SUPPORT
CUSTOMER SUPPORT MANAGERS
COMMERCE PAYMENT PROCESSING CMRS/CMLSt
SYSTEM MONITOR
ACCOUNT REFUND APPLICATION
QA ENVELOPE UPLOAD APPLICATION
QA ENVELOPE SCAN APPLICATION

FIG. 5

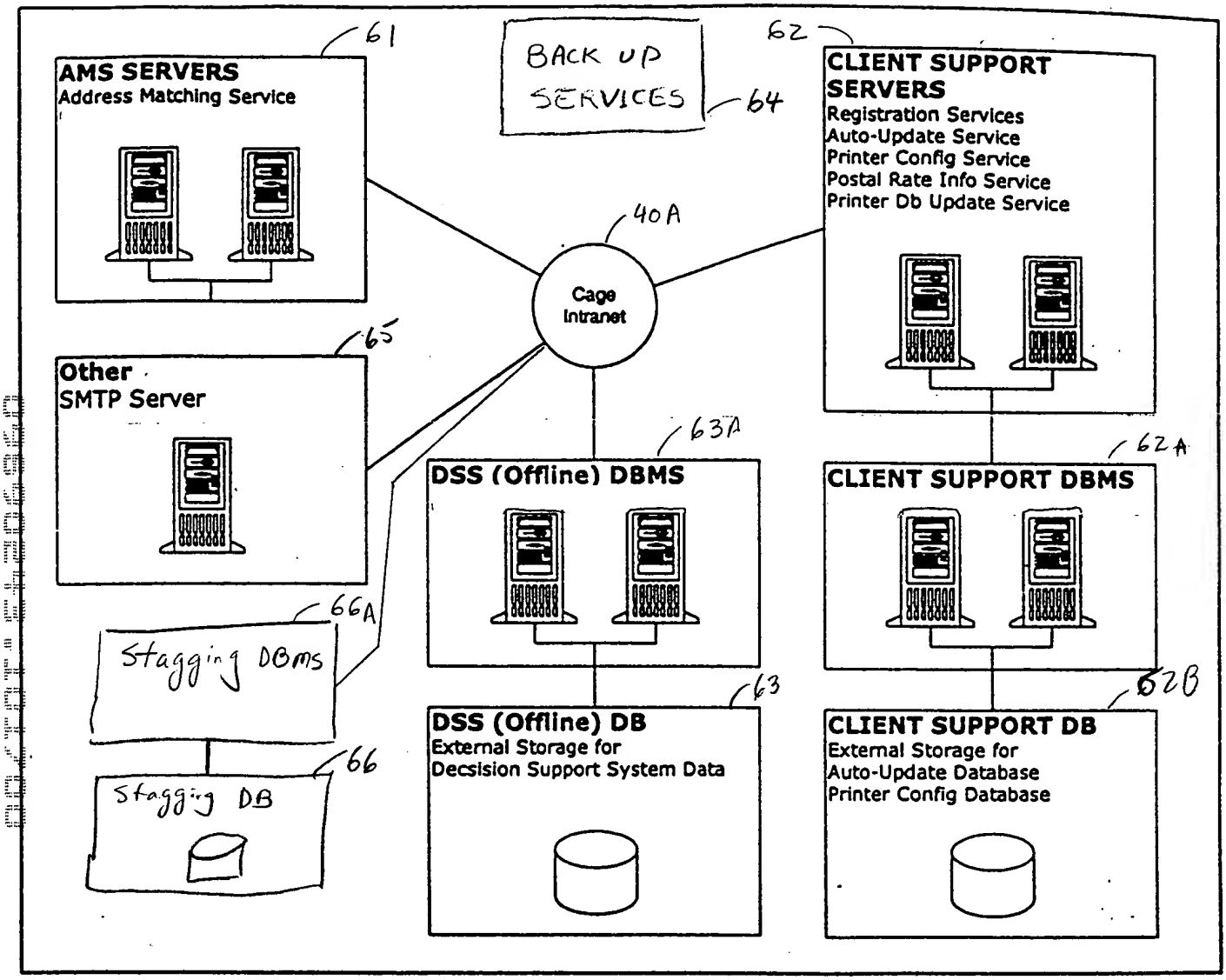

61
AMS SERVERS
Address Matching Service
BACK UP SERVICES
64
62
CLIENT SUPPORT SERVERS
Registration Services
Auto-Update Service
Printer Config Service
Postal Rate Info Service
Printer Db Update Service
40A
Cage Intranet
65
Other
SMTP Server
63A
DSS (Offline) DBMS
62A
CLIENT SUPPORT DBMS
66A
Stagging DBms
63
DSS (Offline) DB
External Storage for
Decsision Support System Data
62B
CLIENT SUPPORT DB
External Storage for
Auto-Update Database
Printer Config Database
66
Stagging DB

FIG. 6

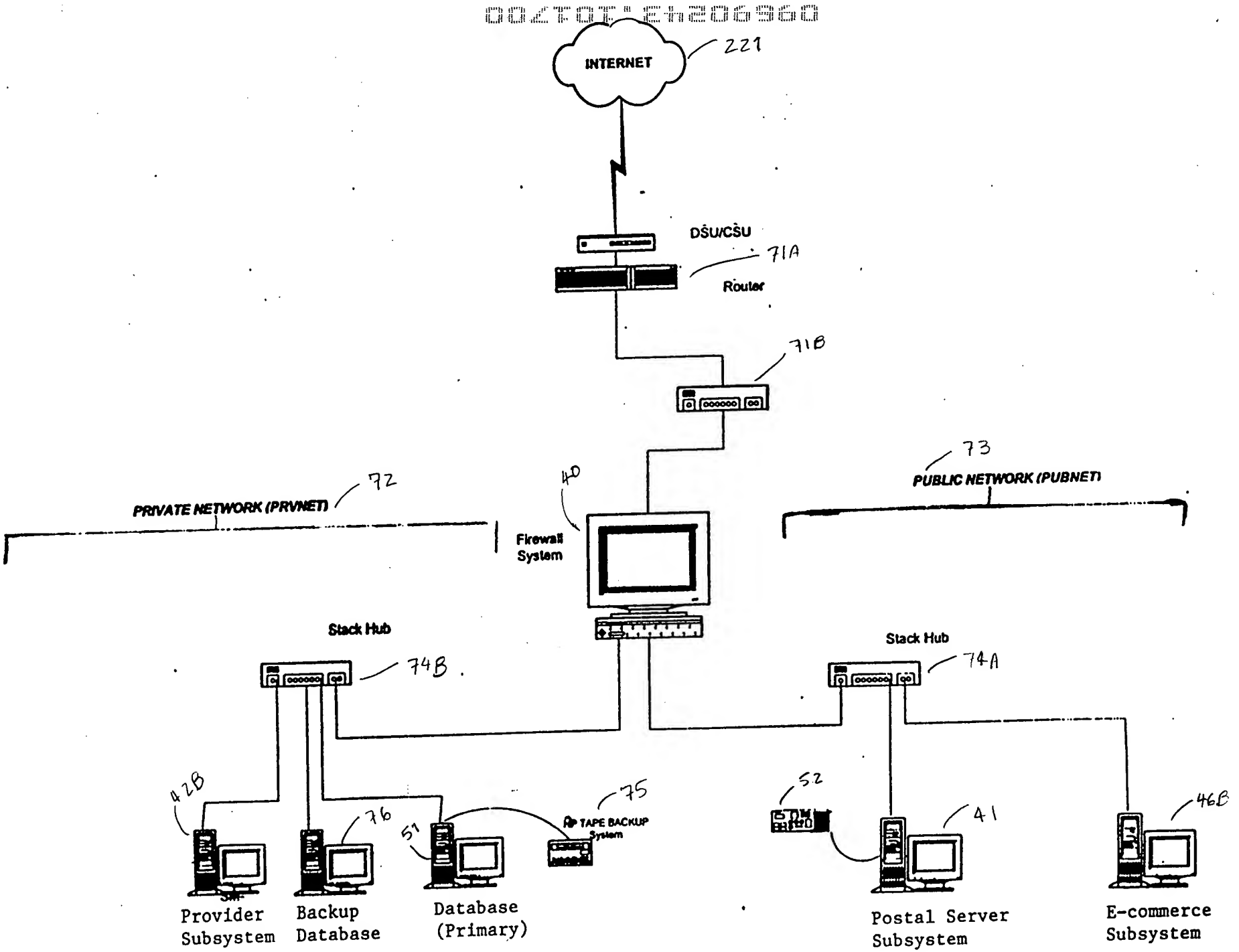
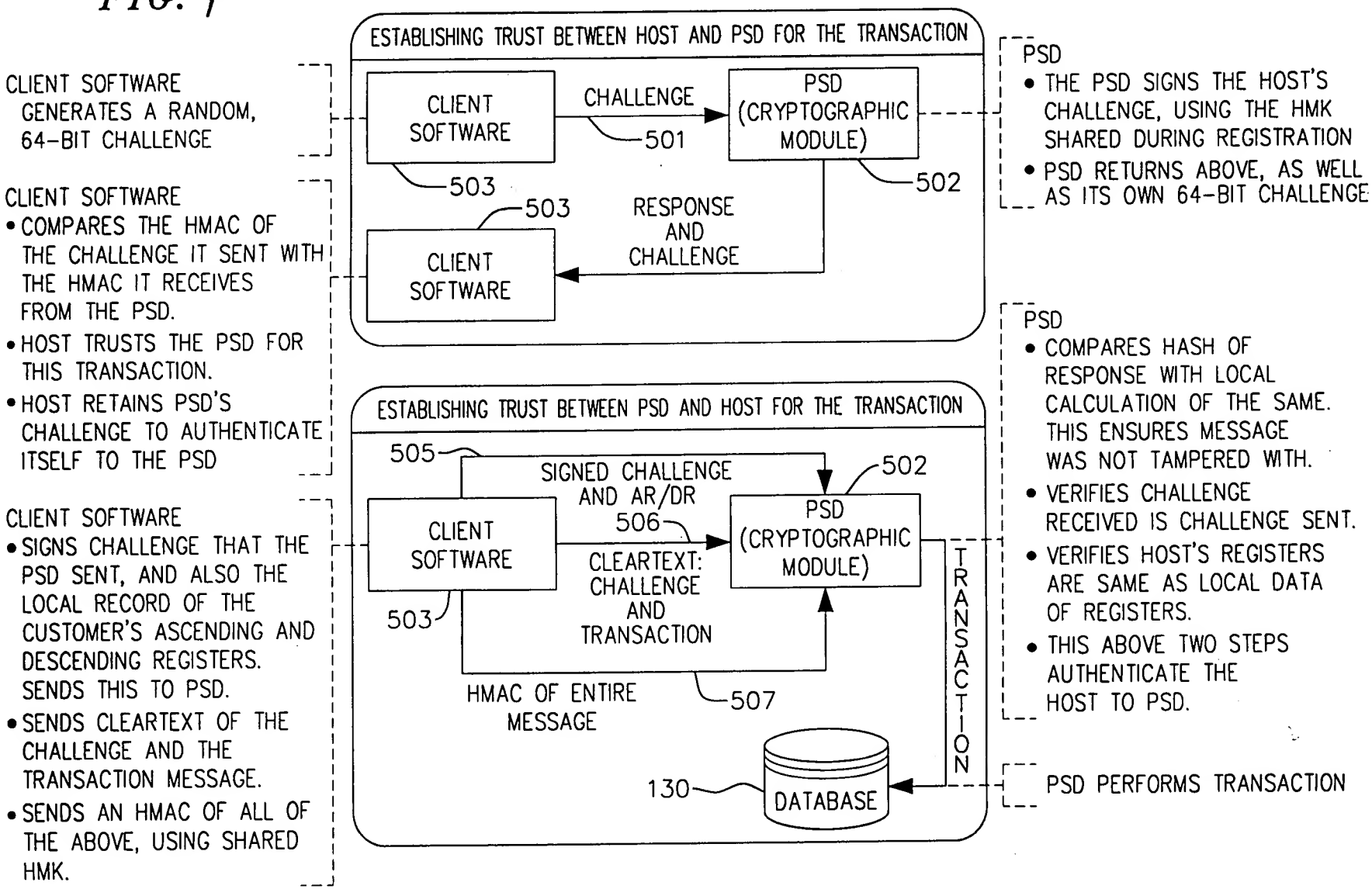

INTERNET
221
DSU/CSU
71A
Router
71B
73
PUBLIC NETWORK (PUBNET)
72
PRIVATE NETWORK (PRVNET)
40
Firewall System
Stack Hub
74B
Stack Hub
74A
42B
76
75
TAPE BACKUP System
51
52
41
46B
Provider Subsystem
Backup Database
Database (Primary)
Postal Server Subsystem
E-commerce Subsystem

FIG. 7


ESTABLISHING TRUST BETWEEN HOST AND PSD FOR THE TRANSACTION
CLIENT SOFTWARE GENERATES A RANDOM, 64-BIT CHALLENGE
CLIENT SOFTWARE
CHALLENGE
501
PSD (CRYPTOGRAPHIC MODULE)
503
502
503
RESPONSE AND CHALLENGE
CLIENT SOFTWARE
PSD
• THE PSD SIGNS THE HOST'S CHALLENGE, USING THE HMK SHARED DURING REGISTRATION
• PSD RETURNS ABOVE, AS WELL AS ITS OWN 64-BIT CHALLENGE
CLIENT SOFTWARE
• COMPARES THE HMAC OF THE CHALLENGE IT SENT WITH THE HMAC IT RECEIVES FROM THE PSD.
• HOST TRUSTS THE PSD FOR THIS TRANSACTION.
• HOST RETAINS PSD'S CHALLENGE TO AUTHENTICATE ITSELF TO THE PSD
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION
505
SIGNED CHALLENGE AND AR/DR
502
CLIENT SOFTWARE
506
PSD (CRYPTOGRAPHIC MODULE)
CLEARTEXT: CHALLENGE AND TRANSACTION
503
TRANSACTION
HMAC OF ENTIRE MESSAGE
507
130
DATABASE
PSD
• COMPARES HASH OF RESPONSE WITH LOCAL CALCULATION OF THE SAME. THIS ENSURES MESSAGE WAS NOT TAMPERED WITH.
• VERIFIES CHALLENGE RECEIVED IS CHALLENGE SENT.
• VERIFIES HOST'S REGISTERS ARE SAME AS LOCAL DATA OF REGISTERS.
• THIS ABOVE TWO STEPS AUTHENTICATE THE HOST TO PSD.
CLIENT SOFTWARE
• SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE CUSTOMER'S ASCENDING AND DESCENDING REGISTERS. SENDS THIS TO PSD.
• SENDS CLEARTEXT OF THE CHALLENGE AND THE TRANSACTION MESSAGE.
• SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED HMK.
PSD PERFORMS TRANSACTION